UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/890,180	01/24/2002	Alexander Medvinsky	018926-003900US	7559

20350 7590 02/08/2006

TOWNSEND AND TOWNSEND AND CREW, LLP
TWO EMBARCADERO CENTER
EIGHTH FLOOR
SAN FRANCISCO, CA 94111-3834

EXAMINER
TO, BAOTRAN N

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 02/08/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/890,180	**Applicant(s)** MEDVINSKY ET AL.
	Examiner Baotran N. To	**Art Unit** 2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on *21 November 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-19* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-19* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. This Office action responds to the application's amendment on 11/21/2005. Claims 1-19 are presented for examination.

Response to Arguments

2. Applicant's arguments filed 11/21/2005 with the respect to Claims 1, 6, 11 and 15 have been fully considered but they are not persuasive.

Applicant argues "Barkan does not teach the step of generating a secret key at the gateway controller."

Examiner respectfully disagrees with this argument above. Barkan clearly discloses the key distribution center creates for each user, a "certificate" that is a digital safe key for each user. The certificate can be used in an open link transaction between users for the secure link establishment. Each certificate includes the user public key, user identification and issue date, all encrypted with the center's private key (col. 4, lines 20-30).

Applicant argues "Barkan does not teach the step of distributing the generated key to both telephone adapters."

Examiner strongly disagrees with this contention. Barkan expressly teaches the key distribution center receives the encryption key request from inquirer and the addresses, and then transmits the desired information after encryption (col. 4, lines 1-5).

Barkan further discloses transferring the encryption key allow to establish a secure communication link between two facilities with encryption machines (col. 7, lines 59 through col. 8, lines 1-2).

Appicant argues "Barkan does not teach the telephone adapters."

Examiner strongly disagrees with this assertion. Barkan explicitly discloses the telephone and fax, cellular/wireless phone, computer communications, remote control/ base station, access control (col. 5, lines 10-13). Furthermore, Barkan clearly teaches user of public key encryption is the PC fax program package offered by Microsoft for the transmission of FAX messages. The FAX may be encrypted using a password or a digital key (col. 3, lines 5-10).

Therefore, the Office action dated on 08/24/2005 for Claims 1, 6, 11 and 15 is maintained.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3. Claims 1-4, 6-9 and 11-19 are rejected under 35 U.S.C. 102(b) as being anticipated by Barkan (EP 0738085 A2) herein referred to as Barkan.

Regarding on Claims 1 and 6, Barkan discloses a method for establishing a secure communication channel in an IP telephony network between a first and a second user, wherein the first user and the second user are coupled to first and second telephony adapters, which in turn, are coupled to first and second gateway controllers, respectively, wherein the gateway controllers control user access to the IP telephony network, and wherein the telephony adapters encrypt and decrypt user information exchanged over the IP telephony network (Fig. 1), the method comprising:

receiving a request at the first gateway controller (key distribution center 11) to establish a secure communication channel (secure communication link) between the first user (facility 1) and the second user (facility 3) (Fig. 1, col. 6, lines 38-40);

generating a secret key (encryption key) at the first gateway controller (col. 3, lines 50-53);

distributing the secret key to the first and second telephony adapters (key management device) over previously established secure connections (col. 3, lines 17-25); and

establishing the secure communication channel between the first user and the second user by encrypting and decrypting information using the secret key (col. 3, lines 17-20).

Regarding on Claim 2, Barkan discloses the limitations as discussed in Claim 1 above. Barkan further discloses wherein the step of generating comprises a step of generating a random number at the first gateway controller to be used as the secret key (col. 14, line 59 and col. 15, lines 1-5).

Regarding on Claim 3, Barkan discloses the limitations as discussed in Claim 1 above. Barkan further discloses wherein the step of generating comprises a step of deriving the secret key at the first gateway controller (col. 15, lines 5-10), wherein the secret key is derived from a signaling key shared between the first telephony adapter and the first gateway controller (col. 15, lines 15-20).

Regarding on Claim 4, Barkan discloses the limitations as discussed in Claim 1 above. Barkan further discloses wherein the step of distributing comprises steps of:

transmitting the secret key from the first gateway controller to the second gateway controller (col. 7, lines 45-55);

transmitting the secret key from the second gateway controller to the second telephony adapter (col. 7, lines 45-50),

transmitting the secret key from the first gateway controller to the first telephony adapter (col. 6, lines 35-40).

Regarding on Claim 7, Barkan further discloses a gateway controller for establishing a secure communication channel in an IP telephony network, the gateway controller coupled between a telephony adapter and a telephony network backbone (Fig. 1), the gateway controller (key distribution center) comprising:

a key creation module (key generating machine) having logic to create a secret key (encryption key) (col. 8, lines 30-35 and Abstract, lines 1-5);

a key storage module (key management controller) coupled to the key creation module and having logic to store the secret key (col. 8, lines 15-20); and

a message processor coupled to the key creation module and the key storage module (col. 8, lines 15-20), and having logic to process messages exchanged between the telephony adapter and the telephony network backbone (Fig. 1, element 111) (col. 7, lines 51-54 and col. 14, lines 15-30), wherein the message processor further comprises:

logic to receive a request to establish a secure communication channel between a first user and a second users the first user couple to the telephony adapter, the second user coupled to a remote telephony adapter (Fig. 1, col. 6, lines 38-40);

logic to distributed the secret key to the telephony adapters over previously established secure connections (col. 3, lines 17-25),

whereby the secure communication channel between the first user and the second user may be established by encrypting and decrypting information using the secret key (col. 3, lines 17-20).

Regarding on Claim 8, Barkan discloses the limitations as discussed in Claim 7 above. Barkan further discloses wherein the key creation module has logic to generate a random number as the secret key (col. 14, line 59 and col. 15, lines 1-5).

Regarding on Claim 9, Barkan discloses the limitations as discussed in Claim 7 above. Barkan further discloses wherein the key creation module has logic to derive the secret key from a signaling key shared with the telephony adapter (col. 8, lines 15-40).

Regarding on Claim 11, Barkan discloses a system for providing encrypted communications in an IP telephony network, said system comprising:

a first cable telephony adapter (facility 1 key management device) (col. 5, lines 53-55);

a first gateway controller (key distribution center 11) coupled with said first cable telephony adapter (col. 6, lines 25-30);

a second cable telephony adapter (facility 3 key management device) (col. 5, lines 52-55);

a second gateway controller (key distribution center 12) coupled with said second cable telephony adapter (col. 7, lines 45-50);

a network coupled with both said first gateway controller and said second gateway controller so as to facilitate communications between said first cable telephony adapter and said second cable telephony adapter wherein said communications are routed via said first gateway controller and said second gateway controller (Fig. 1, col. 5, line 52 through col.12, line 18), wherein said first gateway controller comprises:

a first key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter (col. 8, lines 15-20).

Regarding on Claim 12, Barkan discloses the limitations as discussed in Claim 11 above wherein said second gateway controller comprises:

a second key creation module configured to generate a secret key for distribution to both said first cable telephony adapter and said second cable telephony adapter for use in encrypted communications between said first cable telephony adapter and said second cable telephony adapter (col. 8, lines 30-35 and Abstract, lines 1-5).

Regarding on Claim 13, Barkan discloses the limitations as discussed in Claim 11 above wherein said first gateway controller further comprises:

a message processor configured to receive an encrypted message from said first cable telephony adapter intended for decryption by said second cable telephony adapter and further configured to forward said encrypted message to said second gateway controller without decrypting said encrypted message (col. 7, lines 51-54 and col. 14, lines 15-30).

Regarding on Claim 14, Barkan discloses the limitations as discussed in Claim 7 above. Barkan further discloses wherein said key creation module is configured to intermittently generate a second secret key and to distribute said second secret key to said first cable telephony adapter and said second cable telephony adapter so as to replace said previously generated secret key (col. 7, lines 45-59 and col. 8, lines 1-40).

Regarding on Claim 15, Barkan discloses a method of establishing secure communications between a first cable telephony adapter and a second cable telephony adapter in a system in which secure communications do not previously exist between said first cable telephony adapter and said second cable telephony adapter, wherein said first cable telephony adapter is coupled with a first gateway controller, said second cable telephony adapter is coupled with a second gateway controller, and a network is coupled with said first gateway controller and said second gateway controller (Fig. 1), said method comprising:

receiving at said first gateway controller (key distribution center 11) a request from said first cable telephony adapter to establish communications between said first cable telephony adapter (facility 1 key management device) and said second cable telephony adapter (facility 3 key management device) (Fig. 1, col. 6, lines 38-40);

generating a secret key (encryption key) at said first gateway controller (key distribution center 11) (col. 16, lines 15-40);

distributing said secret key to said second gateway controller via a secure communication (secure communication link) (col. 7, lines 45-55);

distributing said secret key from said second gateway controller (key distribution center 12) to said second cable telephony adapter (col. 7, lines 45-50);

distributing said secret key from said first gateway controller to said first cable telephony adapter (col. 6, lines 35-40).

Regarding on Claim 16, Barkan discloses the limitations as discussed in Claim 15 above. Barkan further discloses comprising:

encrypting a message at said first cable telephony adapter with said secret key (col. 6, lines 30-35);

sending said encrypted message to said first gateway controller (col. 9, lines 45-50);

receiving said encrypted message at said first gateway controller (col. 6, lines 25-40);

forwarding said encrypted message from said first gateway controller to said second gateway controller without decrypting said encrypted message (col. 10, lines 45-55).

Regarding on Claim 17, Barkan discloses the limitations as discussed in Claim 15 above. Barkan further discloses comprising:

receiving said encrypted message at said second gateway controller (col. 10, lines 45-50);

forwarding said encrypted message from said second gateway controller to said second cable telephony adapter without decrypting said message (col. 10, lines 35-55);

decrypting said encrypted message at said second cable telephony adapter (col. 15, lines 17-20).

Regarding on Claim 18, Barkan discloses the limitations as discussed in Claim 15 above. Barkan further discloses comprising;

encrypting a message at said first cable telephony adapter with said secret key (col. 6, lines 30-35);

sending said encrypted message to said first gateway controller (col. 9, lines 45-50);

receiving said encrypted message at said first gateway controller (col. 6, lines 25-40);

routing said encrypted message from said first gateway controller to said second cable telephony adapter (col. 12, lines 5-15).

Regarding on Claim 19, Barkan discloses the limitations as discussed in Claim 15 above. Barkan further discloses comprising:

receiving said encrypted message at said second cable telephony adapter (col. 15, lines 15-17);

decrypting said encrypted message at said second cable telephony adapter with said secret key (col. 15, lines 17-20).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 5 and 10 are rejected under 35 U.S.C. 103(a) as being unpatentable over Barkan as applied to claims 1 and 7 above, and further in view of Ganesan (U.S. Patent 5,535,276) herein referred to as Ganesan.

Regarding on Claim 5, Barkan discloses the limitations as discussed in Claim 1 above. Barkan does not disclose receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and providing the secret key to the law enforcement server.

However, Ganesan discloses receiving a request at the first gateway controller to provide the secret key to a law enforcement server; and providing the secret key to the law enforcement server (Fig. 2, col. 17, lines 25-40).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have incorporated Ganesan's invention with Barkan to provide the secret key to a law enforcement server with the motivation to allow the government access to messages.

Regarding on Claim 10, Barkan discloses the limitations as discussed in Claim 7 above. Barkan further discloses wherein the key storage module has logic to encrypt the secret key before storage (col. 10, lines 20-25), but Barkan explicitly does not disclose using a public/private key pair belonging to law enforcement.

However, Ganesan discloses using a public/private key pair belonging to law enforcement (col. 9, lines 40-55).

Therefore, it would have been obvious to one of ordinary skill in the art at the time the invention was made to have modified Ganesan's invention with Barkan to use a public/private key pair belonging to law enforcement with the motivation to allow the law enforcement to check on communications between users.

Conclusion

5. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Baotran N. To whose telephone number is 571-272-8156. The examiner can normally be reached on Monday-Friday from 8:00 to 4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Baotran To
01/24/2006

KIM VU
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100